CLAIMS

1.   A method for providing a user device with a set of access
codes, the method comprising:
          in the user device, storing an encryption key and an
5   identification code, and sending a message containing the
identification code to a server via a communications network;
          in the server, storing an encryption key corresponding to
the key stored in the user device, allocating the set of
access codes on receipt of the identification code from the
10 user device, performing a look up function based on the
identification code received in the message to retrieve the
key from storage, encrypting the set of access codes using the
retrieved key to produce an encrypted set, and sending a
message containing the encrypted set to the user device via
15 the network; and,
          in the user device, decrypting the encrypted set
received from the server using the key in storage, and storing
the decrypted set of access codes for use by a user of the
user device; and,
20   upon the number of unused access codes reaching a
predetermined threshold, in the server, sending a message
containing a new set of access codes to the user device via
the network; and,
          in the user device, storing the new set for use by a user
25 of the user device.

2.   A method as claimed in claim 1, further comprising:
          in the user device, tracking the access codes used by the
user, generating a request in response to the number of unused
access codes reaching a predetermined threshold, and sending a
30 message containing the request to the server; and,
          in the server, sending the message containing the new set
of access codes on receipt of the request.

3.   A method as claimed in claim 1, further comprising: in
the server, tracking the access codes used by the user, and
sending the message containing the new set of access codes to
the user device in response to the number of unused access
5 codes reaching a predetermined threshold.

4.   A method as claimed in claim 1, further comprising:
     in the server, generating a new key, encrypting the new
key with the previous key, and sending a message containing
the encrypted new key to the user device via the network; and,
10   in the user device, decrypting the new key received from
the server using the previous key, and storing the decrypted
new key in place of the previous key.

5.   A method as claimed in claim 4, further comprising:
     in the server, encrypting a new set of access codes with
15 the new key to produce a new key encrypted set, and sending a
message containing the new key encrypted set to the user
device via the network; and,
     in the user device, decrypting the new key encrypted set
using the new key, and storing the decrypted new set for use
20 by a user of the user device.

6.   A method as claimed in claim 1, further comprising:
     in the user device, generating a public/private key pair,
and sending a message containing the public key of the pair to
the server via the network;
25   in the server, generating a session key, encrypting the
set of access codes with the session key to produce a session
key encrypted set, encrypting the session key with the public
key to produce an encrypted session key, sending a message
containing the session key encrypted set and the encrypted
30 session key to the user device via the network; and,
     in the user device, decrypting the encrypted session key
with the private key of the pair to recover the session key,
decrypting the session key encrypted set with the recovered
session key to recover the set, and storing the decrypted set
35 for use by a user of the user device.

AMENDED SHEET

7.   A method for providing a user device with a set of access codes, the method comprising, in the user device:

storing an encryption key and an identification code;

5   sending a message containing the identification code to a server via a communications network;

receiving from the server a message containing the set of access codes encrypted with the key;

decrypting the received set of access codes using the key
10 in storage; and,

storing the decrypted set of access codes for use by a user of the user device.

upon the number of unused access codes reaching a predetermined threshold, receiving from the server a message
15 containing a new set of access codes; and,

in the user device, storing the new set for use by a user of the user device.

8.   A method as claimed in claim 7, further comprising: in the user device, tracking the access codes used by the user,
20 generating a request in response to the number of unused access codes reaching a predetermined threshold, and sending a message containing the request to the server.

9.   A method as claimed in claim 7, further comprising, in the user device:
25 decrypting a new key received from the server using the previous key; and,

storing the decrypted new key in place of the previous key.

10.   A method as claimed in claim 9, further comprising, in
30 the user device:

receiving from the server a message containing a new key encrypted set of access codes via the network;

decrypting the new key encrypted set using the new key; and,

AMENDED SHEET

storing the decrypted new set for use by a user of the
user device.

11.   A method as claimed in claim 7, comprising, in the user
device:

5   generating a public/private key pair;
         sending a message containing the public key of the pair
to the server via the network;
         receiving a message containing a session key encrypted
set of access codes and a public key encrypted session key
10 from the server via the network;
         decrypting the public key encrypted session key with the
private key of the pair to recover a session key encrypted set
and a corresponding session key;
         decrypting the session key encrypted set with the
15 recovered session key to recover the set; and,
         storing the decrypted set for use by a user of the user
device.

12.   A computer program element comprising computer program
code mean when loaded in a processor of a user device,
20 configures the processor to perform a method as claimed in any
of claims 7 to 11.

13.   A method for providing a user device with a set of access
codes, the method comprising, in a server for communicating
with the user device via a network:
25   storing an encryption key corresponding to an encryption
key stored in the user device;
         allocating the set of access codes to the user device on
receipt of a message containing an identification code from
the user device via the network;
30   performing a look up function based on the identification
code received in the message to retrieve the key from storage;
         encrypting the set of access codes using the retrieved
key to produce an encrypted set; and,
         sending a message containing the encrypted set to the
35 user device via the network; and,

upon the number of unused access codes reaching a predetermined threshold, sending a message containing a new set of access codes to the user device via the network.

14. A method as claimed in claim 13, further comprising, in
5 the server:
    generating a new key, encrypting the new key with the previous key; and,
    sending a message containing the encrypted new key to the user device via the network; and,

10 15. A method as claimed in claim 14, further comprising, in
    the server:
    encrypting the new set of access codes with the new key to produce a new key encrypted set of access codes.

16. A method as claimed in claim 13, further comprising, in
15 the server:
    receiving a message containing a public key of a public/private key pair from the user device;
    generating a session key;
    encrypting the set of access codes with the session key
20 to produce a session key encrypted set;
    encrypting the session key with the public key to produce a public key encrypted session key; and,
    sending a message containing the session key encrypted set and the public key encrypted session key to the user
25 device via the network.

17. A computer program element comprising computer program code means when loaded in a processor of a server computer system, configures the processor to perform a method as claimed in any of claims 13 to 16.

30 18. A method as claimed in any of claims 1 to 16, wherein the access codes are one time authentication codes.

AMENDED SHEET

19. A method as claimed in any of claims 1 to 16, or 18, wherein the network comprises a wireless communication network.

20. A method as claimed in claim 19, wherein the user device
5 comprises one of a mobile phone, a personal digital assistant, and a smart card.

21. A method as claimed in claim 19, wherein the messages are SMS messages.

22. Apparatus for providing a user with a set of access codes,
10 the apparatus comprising: a user device; and, server for communicating with the user device via a communications network; the user device comprising means for storing an encryption key and an identification code, and means for sending a message containing the identification code to the
15 server via the network; the server comprising means for storing an encryption key corresponding to the key stored in the user device, means for allocating the set of access codes on receipt of the identification code from the user device, means for performing a look up function based on the
20 identification code received in the message to retrieve the key from storage, means for encrypting the set of access codes using the retrieved key to produce an encrypted set, and means for sending a message containing the encrypted set to the user device via the network and for sending upon the number of
25 unused access codes reaching a predetermined threshold, a message containing a new set of access codes to the user device via the network; and, in the user device, storing the new set for use by a user of the user device.
and, the user device further comprising means for decrypting
30 the encrypted set received from the server using the key stored in the user device, and means for storing the decrypted set of access codes for use by the user.

23. Apparatus as claimed in claim 22, wherein the server
further comprises means for generating a new key, means for
encrypting the new key with the previous key, and means for
sending a message containing the encrypted new key to the user
5 device via the network, and wherein the user device further
comprises means for decrypting the new key received from the
server using the previous key, and means for storing the
decrypted new key in place of the previous key.

24. Apparatus as claimed in claim 23, wherein the server
10 further comprises means for encrypting the new set of access
codes with the new key to produce a new key encrypted set; and
means for sending a message containing the new key encrypted
set to the user device via the network, and wherein the user
device further comprises means for decrypting the new key
15 encrypted set using the new key, and means for storing the
decrypted new set for use by a user of the user device.

25. Apparatus as claimed in claim 22, further comprising in
the user device, means for storing the new set for use by a
user of the user device.

20 26. Apparatus as claimed in claim 25, further comprising: in
the user device, means for tracking the access codes used by
the user, means for generating a request in response to the
number of unused access codes reaching a predetermined
threshold, and means for sending a message containing the
25 request to the server; and, in the server, means for sending
the message containing the new set of access codes on receipt
of the request.

27. Apparatus as claimed in claim 25, further comprising: in
the server, means for tracking the access codes used by the
30 user, and means for sending the message containing the new set
of access codes to the user device in response to the number
of unused access codes reaching a predetermined threshold.

AMENDED SHEET

ART 34 AMDT

28. Apparatus as claimed in claim 25, further comprising: in
the user device, means for generating a request in response to
a manual input from the user, and means for sending a message
containing the request to the server; and, in the server,
5 means for sending the message containing the new set of access
codes on receipt of the request.

29. Apparatus as claimed in claim 22, wherein the user device
further comprises means for generating a public/private key
pair and means for sending a message containing the public key
10 of the pair to the server via the network; wherein the server
further comprises means for generating a session key, means
for encrypting the set of access codes with the session key to
produce a session key encrypted set, means for encrypting the
session key with the public key to produce a public key
15 encrypted session key, and means for sending a message
containing the session key encrypted set and the public key
encrypted session key to the user device via the network; and,
wherein the user device further comprises means for decrypting
the public key encrypted session key with the private key of
20 the pair to recover the session key, means for decrypting the
session key encrypted set with the recovered session key to
recover the set, and means for storing the decrypted set for
use by a user of the user device.

30. Apparatus as claimed in any of claims 22 to 29, wherein
25 the access codes are one time authentication codes.

31. Apparatus as claimed in any of claims 22 to 28, wherein
the network comprises a wireless communication network.

32. Apparatus as claimed in claim 31, wherein the user device
comprises one of a mobile phone, a personal digital assistant,
30 and a smart card.

33. Apparatus as claimed in claim 31, wherein the messages
are SMS messages.

34. A user device for receiving a set of access codes from a
server via a communications network, the device comprising:
means for storing an encryption key and an identification
code; means for sending a message containing the

5   identification code to a server via a communications network;
means for receiving from the server a message containing the
set of access codes encrypted with the key; means for
decrypting the received set of access codes using the key in
storage; and, means for storing the decrypted set of access

10   codes for use by a user of the user device; and
means for receiving upon the number of unused access codes
reaching a predetermined threshold from the server a message
containing a new key encrypted set of access codes via the
network.

15   35. A user device as claimed in claim 34, further comprising:
means for decrypting a new key received from the server using
the previous key; and, means for storing the decrypted new key
in place of the previous key.

36. A user device as claimed in claim 35, further comprising:

20   means for decrypting the new key encrypted set using the new
key; and, means for storing the decrypted new set for use by a
user of the user device.

37. A user device as claimed in claim 34, further comprising:
means for generating a public/private key pair; means for

25   sending a message containing the public key of the pair to the
server via the network; means for receiving a message
containing a session key encrypted set of access codes and a
pub__c key encrypted session key from the server via the
net__rk; means for decrypting the public key encrypted session

30   key with the private key of the pair to recover the session
key; means for decrypting the session key encrypted set with
the_recovered session key to recover the set; and, means for
storing the decrypted set for use by a user of the user
device.

AMENDED SHEET

38.   A server for providing a user device with a set of access
codes via a communications network, the server comprising:
means for storing an encryption key corresponding to an
encryption key stored in the user device; means for allocating
5 the set of access codes to the user device on receipt of a
message containing an identification code from the user device
via the network; means for performing a look up function based
on the identification code received in the message to retrieve
the key from storage; means for encrypting the set of access
10 codes using the retrieved key to produce an encrypted set;
and, means for sending a message containing the encrypted set
to the user device via the network, means for sending upon the
number of unused access codes reaching a predetermined
threshold a message containing the new set of access codes to
15 the user device via the network.

39.   A server as claimed in claim 38, further comprising:
means for generating a new key, encrypting the new key with
the previous key; and, means for sending a message containing
the encrypted new key to the user device via the network; and,

20 40.   A server as claimed in a claim 39, further comprising:
means for encrypting the new set of access codes with the new
key to produce a new key encrypted set.

41.   A server as claimed in claim 38, further comprising:
means for receiving a message containing a public key of a
25 public/private key pair from the user device; means for
generating a session key; means for encrypting the set of
access codes with the session key to produce a session key
encrypted set; means for encrypting the session key with the
public key to produce a public key encrypted session key; and,
30 means for sending a message containing the session key
encrypted set and the public key encrypted session key to the
user device via the network.

AMENDED SHEET